1. What is an IDOR?

An **IDOR** (Insecure Direct Object Reference) vulnerability is a type of access control flaw that occurs when an application exposes internal objects (like files, database records, or URLs) without proper authorization checks. This allows users to directly access, modify, or delete resources they shouldn't have access to by simply altering a parameter or identifier in a request. IDOR vulnerabilities are part of the **Broken Access Control** category, and they often arise when developers overlook robust permission validation.

How IDOR Works

Imagine a web application that allows users to view their profile by navigating to a URL like:

```
https://example.com/profile?user_id=123
```

If the application does not properly check permissions, a user could change the `user_id` parameter in the URL to another user's ID, like `user_id=456`, and access or modify that user's profile data.

Example Scenarios of IDOR

1. **File Access**: Accessing documents or resources that belong to other users, such as `/download?file_id=111`, and changing `file_id` to `112`.
2. **User Account Manipulation**: Changing parameters like `order_id` or `user_id` to view or modify another user's orders or account details.
3. **Unauthorized Actions**: Exploiting an IDOR to perform unauthorized actions, such as changing the status of another user's account by altering request parameters.

Why IDOR is Dangerous

IDOR vulnerabilities can lead to **data breaches**, **privilege escalation**, and **unauthorized modifications**. In severe cases, an attacker can gain full access to sensitive information across an application or cause widespread harm by accessing and modifying critical resources.

Preventing IDOR

- **Implement Strong Access Control**: Always verify the user's permissions on server-side before granting access to any resource.
- **Use Random Identifiers**: Instead of sequential IDs (like 123, 124), use unique and non-guessable identifiers (like UUIDs).
- **Regular Security Testing**: Conduct routine pentesting and code reviews, specifically looking for broken access control issues.

IDOR is a critical vulnerability in web applications, and staying vigilant with access controls and testing can mitigate the risk.